

Page Denied

DCI/IC 5348-82

OGC 82-02693
17 March 1982

Seg 3

MEMORANDUM FOR: Director, Intelligence Community Staff
Deputy Director for Administration
Deputy Director for Operations
Deputy Director for Science and Technology
Deputy Director for Intelligence
Comptroller
Inspector General
Director of Personnel
Chairman, National Intelligence Council
Director, External Affairs
Director of Security
Chairman, SECOM

FROM:


Associate General Counsel for
Intelligence Community Affairs

25X1

SUBJECT:

Draft Interdepartmental Report on the Problem
of Unauthorized Disclosures of Classified
Information

1. The subject report is provided for your review and comment. The interdepartmental group which will submit the report to the Attorney General was commissioned by the 2 February 1982 memorandum of the Assistant to the President for National Security Affairs concerning implementatin of NSDD-19.

2. Due to the deadline imposed by the Department of Justice, we need to receive any comments you wish to have considered as part of our written submission by noon on Friday, 19 March. Comments received after that date will be considered for discussion at the interdepartmental group's next meeting on 23 March.

DOJ Review
Completed.

25X1

Attachment.



U.S. Department of Justice
Civil Division

General Counsel

Deputy Assistant Attorney General

Washington, D.C. 20530

March 16, 1982


MEMORANDUM FOR:

Daniel W. McGovern
Deputy Legal Adviser
Department of State

Jordan Luke
Assistant General Counsel
Department of the Treasury

Kathleen A. Buck
Assistant General Counsel
Department of Defense

James W. Culpepper
Deputy Assistant Secretary
for Security Affairs
Department of Energy


Deputy General Counsel
Central Intelligence Agency

25X1

Richard C. Morris
Special Assistant to the Assistant to
the President for National Security Affairs

SUBJECT

: Draft Report for Interdepartmental Group
on Unauthorized Disclosure of Classified
Information

Enclosed for your review and comment is the draft report, except for Parts B and D. The Executive Summary (Part A) and recommended National Security Decision Directive (Part G) should provide a general indication of what the missing parts will look like.

Any written coments that I receive by 9:00 a.m. on Monday, March 22, will be reproduced and circulated to the group that morning. At that time I shall also circulate a second draft of the report for discussion at our March 23 meeting. That meeting will take place at 3:00 p.m. in Room 6744 at the Department of Justice.

I would encourage you to limit circulation of the present draft report. The March 22 draft should be suitable for more extensive circulation.

Richard K. Willard

Richard K. Willard
Deputy Assistant Attorney General
Civil Division

Attachments

cc: L. Britt Snider
Peter Rusthoven
Robert Kimmitt

Table of Contents

- A. Executive Summary
- B. Nature of the Problem and Scope of Report
- C. Laws Pertaining to Unauthorized Disclosures
- D. Protective Security Programs
- E. Past Experience with Leak Investigations
- F.. Proposed New Approach to Leak Investigations
- G. Draft National Security Decision Directive

TAB A

DRAFT 3/16/82

Tab A

EXECUTIVE SUMMARY

Unauthorized disclosure of classified information is a longstanding problem that has increased in severity over the past decade. This problem has resisted efforts at solution under a number of Administrations. Yet the protection of national security information remains a fundamental constitutional duty of the President. The current epidemic of unauthorized disclosures has gravely compromised the security of the United States. We must seek more effective means to prevent, deter, and punish unauthorized disclosures. At the same time, we must recognize that this complex problem is unlikely to be solved easily or quickly.

The scope of this report is limited to unauthorized disclosures of classified information where there is no apparent involvement of a foreign power. Such disclosures primarily occur through media "leaks" by anonymous government employees, or in publications and statements by former employees. Beyond the scope of this report are the following kinds of disclosures:

- disclosures of classified information to foreign powers or their agents, which is espionage in the classic sense;
- authorized disclosures of classified information by government officials who are not publicly identified;
- leaks of unclassified information; and
- compromise of classified information through negligence.

Although some of the foregoing kinds of disclosures also present serious problems, we have limited the scope of this report in order to produce a more comprehensible set of recommendations.

Laws Pertaining to Unauthorized Disclosures

The unauthorized disclosure of classified information has been specifically prohibited by a series of Executive orders dating back at least to 1940. Such disclosures also violate numerous more general standards of conduct for government employees based on statutes and regulations. It

-2-

is clear that any government employee may be discharged or otherwise disciplined for making unauthorized disclosures of classified information. Moreover, in virtually all cases the unauthorized disclosure of classified information potentially violates one or more federal criminal statutes.

However, there is no single statute that makes it a crime as such for a government employee to disclose classified information without authorization. With the exception of certain specialized categories of information, the government must prosecute unauthorized disclosures as violations of the Espionage Act. Such prosecutions have not been successfully undertaken because of a variety of procedural and substantive problems.

Therefore, it would be helpful if Congress enacted a law providing criminal penalties for government employees who, without authorization, disclose information that is properly classified pursuant to statute or Executive order. Such a law would be appropriate in view of the substantial body of criminal statutes punishing unauthorized disclosure of other kinds of sensitive information by government employees, such as banking, agricultural and census data. Classified national security information would seem to be deserving of at least the same degree of protection.

A promising development in recent years has been the judicial recognition that the government may enforce secrecy agreements through civil litigation. Many government employees sign secrecy agreements as a condition of employment with intelligence agencies or access to classified information. In a series of cases culminating in the Supreme Court's 1980 decision in United States v. Snepp, the Justice Department has obtained injunctions and monetary remedies from individuals who seek to publish classified information in violation of their secrecy obligations. Such civil litigation avoids many of the procedural problems that would be encountered in criminal prosecutions. The effectiveness of this program would be increased by greater use of properly drafted secrecy agreements.

Protective Security Programs

The overall effectiveness of the government's programs for safeguarding classified information undoubtedly affects the frequency of leaks. Tight security measures--including limiting access to classified information to those with a real "need to know"--reduce the opportunities for unauthorized disclosure. By contrast, lax security measures may encourage leaks by causing employees to believe that classified information does not really require protection.

-3-

As a general rule, protective security programs serve a number of objectives besides prevention of unauthorized disclosures, and therefore this report does not consider these programs in great detail. The following observations are made:

- Security education programs could be improved, especially for senior officials.
- Better controls on copying and circulation of classified documents would reduce dissemination and aid the task of investigating leaks.
- The federal personnel security program under E.O. 10450 and implementing regulations is in serious need of revision and updating.

The first two problems are currently being addressed by the Security Committee established by the Director of Central Intelligence. The last problem should be addressed by an interdepartmental group under the leadership of the Department of Justice, in consultation with the Office of Personnel Management.

We also considered whether there should be a government-wide program to regulate or limit contacts between government officials and media representatives. Such contacts, especially when they occur on a frequent and informal basis, may give rise to deliberate as well as negligent disclosures of classified information. Therefore, the problem of regulating media contacts is best left to each department or agency.

Past Experiences with Leak Investigations

Leaks are extremely difficult to investigate because they involve a consensual transaction. Both the leaking official and the receiving journalist have a strong incentive to conceal the source of the information.

Leak investigations do not focus on the receiving journalist for a variety of reasons. Rarely is there sufficient probable cause to justify a search or electronic surveillance of the journalist. The use of other investigative techniques (informants, physical surveillance) may raise First Amendment concerns. Finally, journalists are unlikely to divulge their sources in response to a subpoena for documents or testimony before a grand jury, and contempt sanctions have not been effective.

-4-

Therefore, leak investigations generally focus on government employees who have had access to the information that is leaked. In most situations, hundreds or thousands of employees have had access to the information, and there is no practical way to narrow the focus of the inquiry. Also, the leaking official is unlikely to confess his offense in response to a simple inquiry. The polygraph can be an effective tool in eliciting confessions, but existing regulations do not permit mandatory use of the polygraph for many employees.

Leaks of classified information constitute a potential violation of the espionage laws and thus fall within the FBI's investigative jurisdiction. (By contrast, many agencies that originate classified information are not authorized to go beyond their own employees in investigating leaks.) However, FBI is reluctant to devote its resources to leak investigations. The burden of such investigations falls almost entirely on the Washington Field Office. Such investigations frequently involve high ranking government officials, who may be uncooperative. Sometimes a time-consuming investigation is undertaken, only to reveal that the source of the leak was a White House or Cabinet official who was authorized to disclose the information. However, it is very rare for an investigation to identify the leaking official, and even rarer that a prosecutable case is developed or even that administrative action is taken against a leaker.

The Criminal Division of the Justice Department has developed the practice of running interference for the FBI by screening leak cases to eliminate those that are unlikely to lead to criminal prosecution. This practice involves the infamous "eleven questions" that agencies are expected to answer when they report leaks to the Criminal Division and that include an advance commitment to provide and declassify such classified information as may be required to support a prosecution.

In summary, the past approach to leak investigations has been almost totally unsuccessful and frustrating to all concerned. There have been frequent disputes between the Justice Department and agencies complaining about leaks. This ineffectual system has led to the belief that nothing can be done to stop leaks of classified information.

Proposed New Approach to Leak Investigations

Until new criminal legislation is enacted, we should recognize that leak investigations are unlikely to lead to successful criminal prosecutions. However, the present system

-5-

would be greatly improved if employees who leak classified information could be identified and fired from their jobs. Therefore, the focus of leak investigations should be on imposition of administrative sanctions except for cases in which exacerbating factors suggest that criminal prosecution should be considered.

We should also recognize that resources are available to investigate only a small fraction of leaks. All leaks should be reported to an interagency group such as the DCI Security Committee (SECOM) for evaluation in light of established criteria. These criteria would include:

- the level of classified information disclosed;
- the resulting damage to national security;
- the extent to which the information was disseminated; and
- the presence of specific "leads" to narrow the focus of investigation.

SECOM should coordinate preliminary internal investigations by agencies to which particular information has been disseminated prior to making a final evaluation of the leak. SECOM would then make a recommendation to Justice as to whether further investigation by FBI is warranted in light of the established criteria. A decision to undertake criminal prosecution would not be required as a prerequisite to FBI investigation; FBI should be specifically authorized to investigate unauthorized disclosures in support of administrative as well as criminal sanctions.

The polygraph is an investigative technique occasionally used in leak investigations. By regulation, most federal employees may only be polygraphed on a voluntary basis. However, there is no constitutional or statutory bar to requiring federal employees to take a polygraph examination as part of an investigation of unauthorized disclosures of classified information. We recommend that existing regulations be changed to permit greater use of the polygraph in leak investigations.

Use of the polygraph is a controversial technique, but security specialists believe it can be effective in situations where a leak investigation turns up a limited number of suspects. Under this approach the polygraph is used sparingly and as a last resort. Such polygraph examinations can be limited to the circumstances of the disclosure being investigated,

-6-

and need not extend to matters of life style that some employees find offensive.

Finally, when investigations identify employees who have disclosed classified information without authority, they should not be let off with a slap on the wrist. The full range of administrative sanctions--including discharge--is available. Most employees have certain procedural rights, including notice, hearing and administrative appeal. However, an agency head who follows proper procedures should have no difficulty in disciplining or discharging leakers. It would be helpful for the MSPB and other administrative bodies to adopt "graymail"-type procedures to protect classified information that may be involved in such situations.

TAB C

LAWS PERTAINING TO UNAUTHORIZED DISCLOSURES1. Executive Orders

The protection of national security information is a fundamental constitutional responsibility of the President. This responsibility is derived from the President's powers as Chief Executive, Commander-in-Chief, and the principal instrument of United States foreign policy. The courts have recognized the constitutional dimension of this responsibility. Chicago & Southern Airlines, Inc. v. Waterman Steamship Corp., 333 U.S. 103, 111 (1948); United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936); United States v. Marchetti, 466 F.2d 1309, 1315 (4th Cir. 1972), cert. denied, 409 U.S. 1063 (1972).

In a number of civil and criminal statutes, Congress has also recognized the President's authority to safeguard national security information through a system of classification. E.g., 5 U.S.C. 552(b)(1) (Freedom of Information Act); 5 U.S.C. 552b(c)(1) (Government in the Sunshine Act); 5 U.S.C. 2302(b)(8)(A) (Whistleblower Statute); 18 U.S.C. 798; 50 U.S.C. 783(b).

In a series of Executive Orders dating back to 1940, Presidents have provided for a system of classification to safeguard national security information. Since these Executive Orders are issued in fulfillment of the President's constitutional responsibilities, they have the force and effect of law. United States v. Marchetti, supra.

The present Executive Order on National Security Information, Executive Order 12065, prohibits the unauthorized disclosure of classified information. It provides that officers and employees of the government shall be subject to appropriate administrative sanctions if they knowingly, willfully and without authorization disclose properly classified information or compromise such information through negligence. Sanctions may include termination of classification authority, reprimand, suspension and removal.

The new draft executive order on national security information provides for similar prohibitions and sanctions and applies to government contractors, licenses and grantees as well as government officers and employees.

2. Criminal Statutes

In analyzing whether unauthorized disclosures of classified information constitute a criminal violation, it is necessary to focus on two categories of criminal statutes, those explicitly prohibiting the disclosure of "classified information," and the so-called "espionage" laws, prohibiting the disclosure of "national defense" information.

a. Classified Information Statutes.

There is no general criminal penalty for the unauthorized disclosure of "classified information" as such; however, several criminal statutes prohibit unauthorized disclosure of

classified information in particular situations. Section 783(b) of Title 50 prohibits government employees from disclosing any classified information to agents of foreign governments or members of communist organizations. However, in light of Congress' consistent refusal to enact a general statute criminalizing the disclosure or publication of classified information, this statute is not likely to be construed to apply to unauthorized disclosures of classified information to the media, even in a case in which the guilty employee has reason to believe that the information may find its way into the hands of an agent of a foreign government or a member of a communist organization as a consequence of its publication.

Section 2277 of Title 42 prohibits government employees and contractors from knowingly communicating "Restricted Data" to any person not authorized to receive such information. "Restricted Data" constitutes classified information concerning atomic weapons and nuclear material. Section 2274 of Title 42 prohibits anyone having possession, access or control over Restricted Data from disclosing it with the intent to injure the United States or secure an advantage to a foreign nation.

In addition to these provisions, 18 U.S.C. 798 prohibits any person from disclosing to any unauthorized person "classified information" concerning communications intelligence and cryptographic activities.

These three sets of provisions are the only criminal statutes that punish the unauthorized disclosure of "classified information" as such.

b. Espionage Laws.

Certain provisions of the espionage laws may also be violated by unauthorized disclosures of sensitive information. The two provisions that would most likely be violated by an unauthorized disclosure of classified information to the media would be 18 U.S.C. 793(d) and (e). Section 793(d) prohibits any person having authorized possession of materials such as documents or photographs "relating to the national defense" or "information" relating to the national defense, if there is "reason to believe" that this information can be used "to the injury of the United States or to the advantage of any foreign nation," from transmitting such materials or information to "any person not entitled to receive it." Similarly, section 793(e) prohibits any person having unauthorized possession or access to such materials or information from transmitting them to other unauthorized persons or failing to deliver them to an authorized government officer or employee.

These provisions have not been used in the past to prosecute unauthorized disclosures of classified information, and their application to such cases is not entirely clear. However, we believe these statutes would be violated by the unauthorized disclosure to a member of the media of

classified documents or information relating to the national defense, although intent to injure the United States or benefit a foreign nation would have to be present where the disclosure is of "information" rather than documents or other tangible materials.

One category of classified information that would probably not be covered by these provisions is information that could not fairly be characterized as "relating to the national defense." In Gorin v. United States, 312 U.S. 19, 28 (1940), the Supreme Court stated that in the context of this statute "national defense" is "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness." Currently, however, information may be classified under Executive Order 12065 if it relates either to "the national defense" or to "the foreign relations" of the United States. Thus, there may be information dealing with "foreign relations" that is properly classifiable under the Executive Order even though it has no bearing on the "national defense" as that phrase was defined in Gorin. If so, the leaking of such information would not be covered by sections 793(d) or (e).

c. Theft of Government Property

18 U.S.C. 641 provides criminal penalties for the unauthorized sale or disposal of "any record, voucher, money, or thing of value of the United States," or the knowing

receipt of the same "with intent to convert it to his use or gain." Convictions under this statute have been upheld in cases where government documents or information have been taken. United States v. Friedman, 445 F.2d 1076 (9th Cir.), cert. denied, 404 U.S. 958 (1971) (conviction for receipt of copy of secret grand jury transcript); United States v. Lambert, 601 F.2d 69 (2d Cir. 1979), cert. denied, 444 U.S. 871 (1979) (convictions for selling information derived from Drug Enforcement Administration computer).

There has been no court test of the applicability of section 641 to unauthorized disclosures of classified information. The Department of Justice has taken the position that prosecution under this statute would be warranted in cases of unauthorized disclosure of classified information. Of course, the substantive applicability of this statute remains to be established. In addition, many of the procedural barriers to successful criminal prosecution would remain.

d. Procedural Barriers to Successful Prosecution

Although there are numerous unresolved questions about the substantive applicability of the foregoing criminal statutes, it is clear that most unauthorized disclosures potentially violate one or all of these statutes. Yet the fact remains that no criminal prosecution has been attempted since Daniel Ellsberg and Anthony Russo were indicted for

leaking the "Pentagon Papers." (Prosecution in that instance was dropped because of governmental misconduct in investigating the case.)

One problem is that leak cases are hard to solve. But even when a suspect is identified, there are numerous procedural barriers to criminal prosecution. These barriers may be analyzed as follows.

First, criminal prosecution serves to confirm the accuracy and sensitivity of the information that has been disclosed. For this reason, many agencies do not want cases prosecuted, so that the accuracy of the disclosed information remains open to question.

Second, criminal prosecution generally requires the Government to prove that the disclosed information was damaging to national security, which may require further public disclosures of classified information. Such proof is required under the espionage statutes and, as a practical matter, is extremely helpful in giving any prosecution jury appeal.

Third, criminal trials are normally conducted before a jury and open to the public. Defendants can threaten to require disclosures of sensitive information in the course of trial -- the so-called "graymail" problem. The Classified Information Procedures Act of 1980 alleviates this problem to some extent but does not solve it entirely.

In summary, the costs of criminal prosecution in terms of harm to national security are likely in many cases to outweigh the benefits of deterrence and respect for the law. Of course, the availability of criminal sanctions is important and should be considered in appropriate cases. But the primary focus of the effort to enforce the laws against unauthorized disclosure should involve administrative and other civil remedies.

3. Civil Remedies

There is no general statute providing for civil penalties or injunctive relief in cases of disclosure of classified information. The absence of such an authorizing statute was noted by several members of the Supreme Court in the "Pentagon Papers" case. However, it appears that a majority of the Court in that case would have permitted the Government, even absent a statute, to enjoin the disclosure of classified information that threatened "direct, immediate, and irreparable damage to our Nation or its people." New York Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart, J., concurring). It is not clear that, as a practical matter, the First Amendment would permit a statute authorizing injunctions under a significantly lower standard.

There are specific statutes providing civil remedies for unauthorized disclosure of nuclear safeguards information. 42 U.S.C. 2167, 2280. The latter statute was successfully

relied upon in obtaining a district court injunction against disclosure of H-bomb information. United States v. Progressive, Inc., 467 F. Supp. 990 (W.D. Wis. 1979), appeal dismissed, 610 F.2d 819 (7th Cir. 1979).

Government employees who engage in unauthorized disclosures of classified information are subject to discipline or discharge for misconduct pursuant to 5 U.S.C. 7513 or equivalent statutes governing specialized employment systems. Applicable standards of conduct are found in Executive Order 12605 and implementing agency regulations prohibiting unauthorized disclosure of classified information, as well as the criminal statutes discussed previously. In addition, unauthorized disclosure of classified information would violate a number of general standards of conduct for government employees. See, e.g., 5 C.F.R. 735.201a(c) (impeding government efficiency); id. 735.201a(e) (making a government decision outside official channels); id. 735.201a(f) (affecting adversely the confidence of the public in the integrity of the government); id. 735.206 (misuse of information not made available to the general public); id. 735.209 (conduct prejudicial to the government).

In addition to the normal administrative sanctions for misconduct, 5 U.S.C. 7532 provides for suspension or removal of certain employees if such action is found to be "necessary in the interest of national security." This statute is implemented in Executive Order 10450 and various agency regulations. These authorities are part of the federal personnel security program and are designed to ensure that persons who are "security risks" do not serve in sensitive positions.

Executive Order 10450 was promulgated in 1953 and seriously needs revision to take into account subsequent court decisions and changes in government organization. The FBI no longer collects information to support the federal personnel security program because of its interpretation of legal constraints and Attorney General guidelines. Because of these shortcomings, the federal personnel security program is practically defunct. However, these shortcomings do not impair the government's ability to discipline or discharge employees for unauthorized disclosure of classified information, since such disclosures constitute misconduct for which normal administrative sanctions are available.

In addition to standards imposed by regulation, many government employees are bound by contractual or fiduciary obligations not to disclose classified information in an unauthorized matter. The Department of Justice has had considerable success in enforcing such obligations in civil litigation against former government employees. Since such persons no longer work for the government, the possibility of administrative sanctions is not a deterrent to their making unauthorized disclosures.

Nondisclosure agreements typically have one or both of the following key provisions. First, the employee agrees never to disclose classified information to an unauthorized person. Second, the employee promises not to publish any material related to classified activities without the express

prior approval of the agency. This second provision is implemented through a mechanism for prepublication review of manuscripts submitted by present or former employees for deletion of classified information.

Key judicial decisions have held that the government is entitled to an injunction against former employees who seek to publish without obtaining clearance pursuant to their obligations to comply with prepublication review programs. Once an agency conducts such prepublication review, it is entitled to delete information that is properly classified, subject to judicial review under the same general standards as applied in FOIA litigation. Finally, a person who publishes in violation of his prepublication review obligations forfeits the right to any profits from his publication, which go into a constructive trust for the benefit of the Government. Snepp v. United States, 444 U.S. 507 (1979); Knopf v. Colby, 509 F.2d 1362 (4th Cir. 1975), cert. denied, 421 U.S. 492 (1975); United States v. Marchetti, 466 F.2d 1309 (4th Cir. 1972), cert. denied, 409 U.S. 1063 (1972). In addition, persons who violate injunctions to comply with nondisclosure obligations risk sanctions for contempt of court, which can include both civil and criminal penalties.

The present policy of the Justice Department, as stated by Attorney General Smith on September 3, 1981, is vigorous and even-handed enforcement of nondisclosure obligations under the Snepp guidelines. This policy statement revoked guidelines issued under the Carter Administration that suggested the Snepp doctrine would only be invoked under limited circumstances.

The availability of civil remedies under the Snepp doctrine suggests that greater attention should be paid to the use of nondisclosure agreements for persons with authorized access to classified information. At a minimum, all such persons should be required to agree never to disclose classified information without authorization. In addition, persons with access to the most sensitive kinds of classified information should be required to agree to a system of prepublication review. At present, nondisclosure agreements are used only in certain agencies, and only CIA and NSA have prepublication review programs.

4. Recommendations for New Legislation

As indicated above, criminal sanctions for unauthorized disclosure of classified information apply only in limited situations involving information concerning the national defense, nuclear weapons and materials, and communications and cryptographic intelligence. Moreover, there are a number of substantive and procedural barriers to successful criminal prosecution in most cases of unauthorized disclosures to members of the media.

To close the gaps in the present law, we recommend the introduction of legislation imposing a criminal penalty for all unauthorized disclosures of classified information by government employees. Such a statute should be simple and general in order to cover all situations, and might provide as follows:

Whoever, being an officer or employee of the United States or a person with authorized access to classified information, discloses, or attempts to disclose, any classified information to a person not authorized to receive it shall be fined not more than \$10,000, or imprisoned not more than three years, or both.

In addition, there should be appropriate definitions of the terms employed. It would be helpful also to have a specific procedure for establishing that information forming the basis for prosecution was in fact properly classified.

An alternative approach to filling the legislative gap would be to amend 18 U.S.C. 641 to make it clear that classified information is government property subject to the penalties of that statute.

Enactment of these or similar provisions would significantly broaden current criminal prohibitions, close the loopholes in present criminal laws and give notice that all unauthorized disclosures of classified information are sufficiently serious to warrant criminal sanctions. They would also alleviate -- but not solve entirely -- certain of the procedural problems likely to be presented in criminal prosecutions.

Present civil statutes and regulations on unauthorized disclosures by government employees are generally adequate, except that they apply only to persons who disclose classified information, not to those who receive it. A person who solicits and receives classified information may be no less responsible for an unauthorized disclosure of such information than the government employee who transmits it, but his conduct is not prohibited by any civil statute. Although we make no recommendation with respect to introduction of legislation providing for civil penalties or other remedies against persons who receive classified information, we believe the subject merits further study as an effective, though probably controversial, method of deterring unauthorized disclosures.

TAB E

Draft 3/16/82

Tab E

PAST EXPERIENCES WITH LEAK INVESTIGATIONS

Leaks of classified information to the media over the past twenty years have been so numerous that only a small fraction could be investigated. These investigations have rarely been successful in identifying the sources of such disclosures. In a number of the cases that were solved, no adverse action was taken against the government employee found to have leaked classified information. There has never been a successful criminal prosecution for leaking classified information.

The Government's dismal record in leak investigations has a number of explanations. By their nature, leaks to the media are difficult to investigate. Self-imposed limitations on the use of certain investigative techniques have made the task even more difficult. The development of more productive approaches to leak investigations has been hampered by misunderstandings between the Justice Department and agencies whose information is leaked. We cannot expect to do better in the future without understanding these problems encountered in the past.

Leaks are consensual transactions in which both parties--the leaking official and the receiving journalist--have a strong incentive to conceal the source of the information.

Both parties are likely to feel a moral justification for the transaction. Many journalists believe they have a duty to make public virtually any secret information they acquire that is newsworthy. To their way of thinking, leaks are part of a sport in which the government tries to keep information secret and they try to find it out. Many journalists believe that any resulting damage to national security is none of their concern.

Similarly, leaking officials may persuade themselves that they are serving the larger national interest by disclosing information that the public has a right to know. Such officials may believe that their policy objectives can be advanced by leaks of classified information, and that there will be no serious harm to national security. Because leaks are so prevalent and leakers are rarely caught, some officials may believe that there is nothing wrong with leaking classified information and that everyone does it.

Agencies whose classified information is leaked have limited powers to conduct investigations. Since most leaks of classified information potentially violate criminal statutes, leak investigations are viewed as potentially involving a law enforcement function. By statute, CIA is prohibited from conducting law enforcement activities. [citations] Similar limitation apply to the military services and the Department of Energy. [citations] Executive Order 12333,

§1.7(d), requires agencies in the intelligence community to report crimes such as leaks of classified information to the Justice Department. Implementing procedures for this provision are expected to limit agency authority to conduct preliminary investigations of such matters generally to interviews of current employees and examination of agency premises. And, as a practical matter, most government agencies do not have the capability to conduct investigations outside their own areas of programmatic responsibility.

These legal and practical limitations have caused the burden of leak investigations to fall on the FBI.

Current Justice Department policy in this regard dates back to the early 1960's. At this time, the FBI was inundated with numerous requests for investigation regarding possible violations of the Espionage Statute as they relate to "Media Leaks" and other mishandling of classified information. This policy is divided into two distinct categories.

Espionage investigations that have no apparent foreign connection are investigated as Espionage-X matters by the FBI. Those investigations regarding the mishandling of classified information, loss of classified information through negligence, or other violations of the Espionage Statutes, which are not related to classified information exposed by the news media, are

investigated upon receipt by the FBI. In these types of investigations, the subject is generally known and the amount of investigation necessary is usually limited. Although the Criminal Division is notified at the inception of these investigations and is kept advised of their status, it does not initiate these investigations. Investigations of these types are rather limited and as stated above, generally require little investigation.

"Media Leaks," however, pose different problems, require more investigation, and are far more numerous. Current policy regarding "Media Leaks" requires that prior to any investigation by the FBI, eleven questions must be answered by the injured agency. These questions are utilized to review existing facts and as a result to limit FBI investigation into these matters. This is necessary due to the vast amount of "Media Leak" investigation requests and the often large number of interviews to be conducted in this type of case.

The responses to the eleven questions are crucial in the early stages of any investigation. These questions can be dissected into three categories:

Questions 1 through 3 pertain to the identification of the article(s) contained in the media and the nature of the classified information contained therein. These questions are:

1. The date and identity of the article or articles disclosing the classified information.

2. Specific statements in the article which are considered classified and whether the data was properly classified.
3. Whether the classified data disclosed is accurate.

This information is necessary to determine if a violation has occurred and to assist the FBI in the investigation, if a violation has occurred.

Responses to questions 4 through 8 serve to identify the sources of the classified information disclosed. These questions are:

4. Whether the data came from a specific document and, if so, the origin of the document and the name of the individual responsible for the security of the classified data disclosed.
5. The extent of official dissemination of the data.
6. Whether the data has been the subject of prior official releases.
7. Whether prior clearance for publication or release of the information was sought from proper authorities.
8. Whether the material or portions thereof, or enough background data has been published officially or in the press to make an educated speculation on the matter possible.

Responses to these questions are a prerequisite for FBI investigations in that they furnish initial leads and may give direction toward the person or persons responsible for the disclosure. Some of these questions further assist in determining if a violation has occurred or if the information could have been obtained from some unclassified source or prior publication which would negate any violation.

Questions 9 through 11 pertain to the prosecutive future of the investigation. These questions are:

9. Whether the data can be declassified for the purpose of prosecution and, if so, the name of the person competent to testify concerning the classification.
10. Whether declassification had been decided upon prior to the publication or release of the data.
11. What effect the disclosure of the classified data could have on the national defense.

The responses to these questions are used by the DOJ to determine if a successful prosecution can be made, should the perpetrator be identified.

If the responses to the above questions indicate that it is not likely that the perpetrator will be identified due to extensive dissemination of the material and/or that successful prosecution cannot be mounted, the Criminal Division will not request that the FBI conduct an investigation. There is, however, an exception to this policy. If, in spite of the responses to the above questions, it can be demonstrated that: the disclosure constitutes a very serious compromise of classified information and it is imperative that the person responsible be identified so as to preclude further disclosures; there is a real possibility that the investigation will be fruitful, e.g. the information had very limited distribution; or the originating agency has not finally decided against declassification for prosecutive purposes, then the Criminal Division will request an FBI investigation.

Although current Justice Department policy requests that complaints concerning "Media Leak" matters be forwarded to the Criminal Division for their review, often the complaint is initially forwarded to the FBI. Also, current policy requests that the injured agency furnish in their initial communication responses to the above questions. Often these agencies omit the responses to the above questions or furnish incomplete responses to them. This procedure causes delay in that the Criminal Division must correspond with the injured agency and request responses to the eleven questions or request more detail regarding the responses which they may have furnished. When the initial complaints are furnished in a complete package, FBI investigation can generally be completed in a very reasonable period of time depending on the number of interviews to be conducted and other investigative considerations.

The Criminal Division receives numerous complaints requesting investigation in "Media Leak" matters which are never referred to the FBI, based upon the above criteria. If all of these complaints were fully investigated, the manpower used would be substantially higher. Many of these complaints involve compromised information which has been accessed by two hundred or more individuals. Obviously, the likelihood of determining the one person responsible for the compromise is extremely remote in this type of situation.

Moreover, a number of legal and policy restrictions limit the ability of FBI to conduct effective leak investigations in cases that are referred. In most cases, the principal "lead" is the published media account of the leaked information. But investigations are generally not permitted to focus on the journalist who published the information. Rarely is there sufficient probable cause to justify use of Fourth Amendment techniques, such as searches or electronic surveillance. Current Department of Justice regulations strictly limit the circumstances under which journalists can be questioned or subpoenaed, and require express prior approval by the Attorney General in each case. 45 Fed. Reg. 76436 (Nov. 19, 1980), to be codified at 28 CFR 50.10. Current informal policies also pretermitt physical surveillance of journalists or the use of information directed at the media in leak cases.

Since FBI cannot investigate journalists who received the classified information, they must focus on government employees who have had access to the information that was leaked. Often hundreds or thousands of employees have had access to the information in question. Unless the information received more limited distribution or there are other "leads" that permit narrowing the scope of inquiry, there is no practical means to conduct an investigation.

Even where the inquiry can be limited to a manageable number of employees, FBI has very little ability to conduct

a successful investigation. The leaking official is unlikely to confess in response to a simple inquiry. High-ranking government officials are frequently uncooperative with leak investigations. The polygraph can be an effective investigatory technique, but most government employees can be polygraphed only if they volunteer for the examination. Moreover, FBI does not have authority to compel any employee to take a polygraph examination or sign an affidavit; such compulsion can only be exercised by agency heads who are often reluctant to discipline high-ranking officials who refuse to cooperate with leak investigations.

In summary, past experience with leak investigations has been largely unsuccessful uniformly frustrating for all concerned. Agencies have been unable to conduct their own non-internal investigations, and yet Justice has been unwilling to permit FBI to investigate most cases. FBI has been asked to investigate a number of leaks without being permitted to use adequate techniques to solve cases. There have been frequent disputes and misunderstandings. This whole system has been so ineffectual as to perpetuate the notion that the government can do nothing to stop leaks of classified information.

TAB F

DRAFT 3/16/82

Tab F

PROPOSED NEW APPROACH TO LEAK INVESTIGATIONS

We should recognize that the threat of criminal prosecution is so illusory as to constitute no real deterrent to the prospective leaker. A more promising approach involves better efforts to identify leakers and the resolution to impose administrative sanctions. For most government employees, a realistic prospect of being demoted or fired for leaking classified information would serve as a deterrent. An effective enforcement program would also reverse the common perception that the Government is powerless to stop leaks of classified information.

The authority and responsibility of agencies that originate classified information should be clarified. All serious leaks should be evaluated and investigated internally by the agency that originated the information. Agencies should adopt procedures to assure that these steps are taken in a timely manner.

An interdepartmental group should be utilized to coordinate agency efforts to conduct preliminary internal investigations for information that has been disseminated outside the originating agency. This group would then evaluate leaks according to established criteria to determine whether further

investigation is warranted. Based upon the collective experience of participating agencies and its own data base, this group would be able to develop proposals for protective security measures and use of special investigative techniques to solve recurring sorts of problems.

Rather than create a new interdepartmental group for this purpose, we recommend using the Security Committee (SECOM) established by the Director of Central Intelligence. SECOM already has responsibility of this nature regarding unauthorized disclosure of intelligence and intelligence sources and methods. It would seem logical to expand the jurisdiction of this group somewhat to include unauthorized disclosure of other kinds of classified information that had been disseminated outside the originating agency. (To the extent that an unauthorized disclosure involved such classified information that had been disseminated only within one agency, the agency could handle the investigation unilaterally.)

SECOM could assist the Justice Department by evaluating and prioritizing leak cases in light of mutually agreeable criteria. This would permit a cooperative rather than confrontational approach to allocation of FBI's investigative resources. Of course, SECOM could not overrule the Attorney General's ultimate authority to control FBI activities. However, it would be in the best interests of all concerned for SECOM's recommendations to be given great weight in deciding which cases FBI would investigate.

FBI's authority should be clarified to include investigation of unauthorized disclosures of classified information for administrative purposes as well as criminal prosecution. In addition, informal and formal restrictions on FBI's use of particular investigative techniques should be revised to permit more effective investigation of those cases that are referred. In particular, existing regulations that preclude use of the polygraph in leak investigations should be modified.

Finally, agency heads should be directed to impose appropriate administrative sanctions in situations where employees are found to have leaked classified information. This will provide assurance to all involved in the investigatory process that their efforts will be worthwhile. The authority is clear to discipline or discharge employees for the unauthorized disclosure of classified information; what is required is the resolution to use this authority in appropriate cases.

TAB G

DRAFT 3/16/82

Tab G

DRAFT NSDD

1. Each agency of the Executive Branch that originates or stores classified information shall adopt internal procedures to safeguard against unauthorized disclosures of classified information in the public media. Such procedures shall at a minimum provide as follows:

a. All persons with authorized access to classified information shall be required to sign a nondisclosure agreement as a condition of access. All such agreements must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States.

b. All persons with authorized access to Sensitive Compartmented Information (SCI) shall be required to sign a nondisclosure agreement as a condition of access to SCI and collateral classified information. All such agreements must include a provision for prepublication review to assure detection of SCI and collateral classified information and, in addition, must be in a form determined by the Department of Justice to be enforceable in a civil action brought by the United States.

c. All persons with authorized access to classified information shall be clearly apprised of the agency's policies regarding contacts with media representatives.

2. Each agency of the Executive Branch that originates or stores classified information shall adopt internal procedures to govern the reporting and investigation of unauthorized disclosures of such information in the public media. Such procedures shall at a minimum provide that:

a. All such disclosures that the agency considers to be seriously damaging to its mission and responsibilities shall be evaluated to ascertain the nature of the information disclosed and the extent to which it had been disseminated.

b. The agency shall conduct a preliminary internal investigation prior to or concurrently with seeking investigative assistance from other agencies.

c. The agency shall maintain records of disclosures so evaluated and investigated.

d. Agencies in the possession of classified information originating with another agency shall cooperate with the originating agency by conducting internal investigations of the unauthorized disclosure of such information.

3. The Security Committee established by the Director of Central Intelligence in DCID 1/11 is authorized to coordinate the reporting, evaluation, and preliminary administrative investigation of unauthorized disclosure of classified information. The Security Committee and the Department of Justice shall jointly develop standards for determining when FBI Investigation is appropriate. The Security Committee shall maintain records of disclosures for analytic purposes.

4. The Federal Bureau of Investigation (FBI) is authorized, pursuant to the direction of the Attorney General, to investigate unauthorized disclosures of classified information for purposes of imposing administrative sanctions as well as criminal prosecution.

5. The Office of Personnel Management and all departments and agencies with employees having access to classified information are directed to revise existing regulations and policies to permit the mandatory use of polygraph examinations in investigating unauthorized disclosures of classified information, so long as the scope of such examinations is limited to the circumstances of the unauthorized disclosure that is being investigated.

6. The Attorney General, in consultation with the Director, Office of Personnel Management, is requested to establish an interdepartmental working group to study the federal personnel security program and recommend appropriate revisions in existing Executive orders, regulations and guidelines.

7. The Assistant to the President for National Security Affairs will monitor implementation of this Directive.